[Docket No. 9]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY
CAMDEN VICINAGE

MICHAEL VOLPE, Plaintiff, v. ABACUS SOFTWARE SYSTEMS CORPORATION, Defendant.	Civil No. 20-10108 (RMB/KMW) **OPINION**

APPEARANCES:

Hinman, Howard & Kattell, LLP
By: Daniel Harris Roseman, Esq.
707 Westchester Ave
Suite 407
White Plains, NY 10604
Attorney for Plaintiff

Archer & Greiner PC
By: Michael S. Horn, Esq.
Court Plaza South
West Wing
21 Main Street, Suite 353
Hackensack, NJ 07081
Attorney for Defendants

BUMB, UNITED STATES DISTRICT JUDGE:

Before the Court is Defendant Abacus Software Systems Corporation's ("Defendant" or "Abacus") Motion to Dismiss Plaintiff Michael Volpe's ("Plaintiff" or "Volpe") Complaint. For the reasons set forth herein, the Court will deny this motion.

I. BACKGROUND

In October 2011, Plaintiff began working for Defendant as an information technology salesperson. [Docket No. 1, at ¶ 8]. At this time, both parties signed an Employment Agreement. [Id. at ¶ 9]. According to the Complaint, Defendant breached this agreement in 2016 by "unilaterally, and without justification or notice, reduc[ing] Plaintiff's salary from $72,000.00 to $50,000.00 per year." [Id. at ¶ 16]. Plaintiff alleges that Defendant breached the agreement because the agreement purportedly required any salary reduction to be in writing and agreed to by both parties, which did not happen. [Id. at ¶¶ 17-18]. Volpe also claims that he repeatedly objected to his salary reduction, and that those objections went unanswered. [Id. at ¶20].

Plaintiff's relationship with his employer then continued to deteriorate. In late 2018, Defendant allegedly stopped reimbursing Plaintiff for certain business expenses. [Id. at ¶ 21]. Previously, Defendant had allegedly reimbursed Plaintiff for all expenses incurred in connection with his employment. [Id. at ¶ 22].

About one year later, in October 2019, Defendant informed Plaintiff that he would be terminated. [Id. at ¶ 24]. Plaintiff alleges that, shortly after this meeting and without notice,

Defendant remotely accessed Plaintiff's personal smart phone and erased "all of the data." [Id. at ¶¶ 25-26].

Defendant allegedly accessed Plaintiff's personal iPhone using a feature called "find my iPhone." [Id. at ¶ 26]. This feature allows a user to remotely delete data from a phone affiliated with their "Apple ID." [Id.]. Although Defendant did not have access to Plaintiff's Apple ID password, Plaintiff alleges that Defendant was able to reset the password using his employer-provided e-mail address, and then delete his personal data. [Id.]. According to Plaintiff, the erased data included "(1) Contacts, (2) Pictures and videos, (3) Data, (4) Applications, (5) Purchases, (6) E-mails, and (7) Settings." [Id. at ¶ 27]. Plaintiff's attempts to recover this data were unsuccessful. [Id. at ¶ 28].

Volpe asserts six causes of action. Plaintiff alleges that Defendant breached his contract by both reducing his pay (Count One) and by refusing to reimburse his business expenses (Count Two). Similarly, Plaintiff alleges that Defendant's actions constitute a breach of the Covenant of Good Faith and Fair Dealing (Count Three). Moreover, Plaintiff claims that Defendant's unilateral reduction of his pay violates N.J.S.A. § 34:11-4.6(b), which requires employers to provide advance notice of changes to employee pay (Count Four). The final two counts arise from Defendant's purportedly improper access to

Plaintiff's phone, which led to the deletion of Plaintiff's data. Volpe claims that this action constitutes a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (Count Five) and the New Jersey Computer Related Offenses Act, N.J.S.A. § 2A:38A-3 (Count Six).

Defendant now moves to dismiss Plaintiff's fifth count, the Computer Fraud and Abuse Act claim. Without this claim, Defendant argues, Plaintiff asserts only state law claims totaling less than $75,000. Moreover, Defendant contends that, after dismissing Plaintiff's only federal claim, the Court should decline to exercise supplemental jurisdiction, and instead dismiss the entire action for lack of jurisdiction. Thus, the Court turns its analysis to Plaintiff's fifth count.

II. STANDARD OF REVIEW

To withstand a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. at 662. "[A]n unadorned, the defendant-unlawfully-harmed-me accusation" does not suffice to survive a

motion to dismiss. Id. at 678. "[A] plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." Twombly, 550 U.S. at 555 (quoting Papasan v. Allain, 478 U.S. 265, 286 (1986)).

In reviewing a plaintiff's allegations, the district court "must accept as true all well-pled factual allegations as well as all reasonable inferences that can be drawn from them, and construe those allegations in the light most favorable to the plaintiff." Bistrian v. Levi, 696 F.3d 352, 358 n.1 (3d Cir. 2012). The Court may consider only the allegations in the complaint, and "matters of public record, orders, exhibits attached to the complaint and items appearing in the record of the case." Oshiver v. Levin, Fishbein, Sedran & Berman, 38 F.3d 1380, 1384 n.2 (3d Cir. 1994) (citing Chester Cnty. Intermediate Unit v. Penn. Blue Shield, 896 F.2d 808, 812 (3d Cir. 1990)).

In addition, Defendant also argues that the Court should dismiss Plaintiff's Computer Fraud and Abuse Act claim pursuant to Fed. R. Civ. P. 12(b)(1). A motion to dismiss for lack of subject matter jurisdiction, pursuant to Fed. R. Civ. P. 12(b)(1), "may be treated as either a facial or factual challenge to the court's subject matter jurisdiction." See Mortensen v. First Fed. Sav. and Loan Ass'n, 549 F.2d 884, 891

(3d Cir.1977). A facial attack "is an argument that considers a claim on its face and asserts that it is insufficient to invoke the subject matter jurisdiction of the court." Const. Party of Pennsylvania v. Aichele, 757 F.3d 347, 358 (3d Cir. 2014). In contrast, a factual attack "is an argument that there is no subject matter jurisdiction because the facts of the case. . . do not support the asserted jurisdiction." Id. Stated differently, "a facial attack contests the sufficiency of the pleadings, whereas a factual attack concerns the actual failure of a plaintiff's claims to comport factually with the jurisdictional prerequisites." Id. (cleaned-up).

When a motion to dismiss presents a facial attack, "the court must only consider the allegations of the complaint and documents referenced therein and attached thereto, in the light most favorable to the plaintiff." In re Schering Plough Corp., 678 F.3d 235, 243 (3d Cir. 2012). In other words, the Court applies "the same standard of review it would use in considering a motion to dismiss under Rule 12(b)(6), i.e., construing the alleged facts in favor of the nonmoving party[,]" when reviewing a facial attack. Const. Party of Pennsylvania, 757 F.3d at 358. But in reviewing a factual attack, the Court "may consider evidence outside the pleadings." Gould Elecs. Inc. v. United States, 220 F.3d 169, 176 (3d Cir. 2000).

III. ANALYSIS

Defendant argues that Plaintiff failed to state a claim under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. The CFAA was designed to create a cause of action against computer hackers. Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 613 (E.D. Pa. 2013). Although the CFAA was originally exclusively a criminal statute, it has been amended to include a civil cause of action. See Computer Abuse Amendments Act of 1994, Pub.L. No. 103-322, § 290001(d), 108 Stat. 1796 (codified at 18 U.S.C. § 1030(g)).

To state a civil CFAA claim, a plaintiff must establish that defendant (1) has accessed a "protected computer;" (2) has done so without authorization or by exceeding such authorization as was granted; (3) has done so "knowingly" and with "intent to defraud"; and (4) as a result has "further[ed] the intended fraud and obtain[ed] anything of value." P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC., 428 F.3d 504, 508 (3d Cir. 2005) (quoting 18 U.S.C. § 1030(a)(4)).

The CFAA further provides that:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).

18 U.S.C. § 1030(g). As relevant here, Plaintiff contends that he has satisfied this requirement by identifying "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value," in violation of § 1030(c)(4)(A)(i)(I). [See Docket No. 13, at 8].

A. Protected Computer

The CFAA defines a protected computer, as relevant here, as a computer "used in or affecting interstate or foreign commerce or communication." § 1030(e)(2)(B). Defendant argues that Plaintiff has not sufficiently alleged that his iPhone was a "protected computer" under this definition. The Court disagrees. Plaintiff has established that his phone was a "smart device" [Docket No. 1, at ¶ 53] capable of accessing the internet. [Id. at ¶¶ 26-27] Moreover, the very nature of Plaintiff's claim concerns remote access of information, via the internet, on his communications device. See United States v. MacEwan, 445 F.3d 237, 245 (3d Cir. 2006) ("the Internet is an instrumentality and channel of interstate commerce.") At this stage in the litigation, Plaintiff's contention is sufficient to establish that the iPhone in question is a protected computer under the meaning of the CFAA.

B. Authorization

"The touchstone of a CFAA claim is the 'unauthorized' access of computers." Christie v. Nat'l Inst. for Newman Stud.,

No. 16-6572 (FLW), 2019 WL 1916204, at *5 (D.N.J. Apr. 30, 2019). A plaintiff must show that a defendant "accessed the computer either 'without authorization' or that [it] 'exceeded authorized access[1].'" Synthes, Inc. v. Emerge Med., Inc., No. CIV.A. 11-1566, 2012 WL 4205476, at *16 (E.D. Pa. Sept. 19, 2012).

Defendant argues that it was authorized to access Plaintiff's smart phone because "Plaintiff specifically gave [Defendant] authority to access his phone," [Docket No. 9-1, at 6] as set forth in the Employee Handbook. According to Defendant, this Handbook states that "[a]ll e-mail and voice mail passwords must be made available to the company at all times." [Id. at 6-7]. In addition, Defendant refers to Plaintiff's Employment Agreement, which requires that its information must be returned whenever Plaintiff's employment terminates.

[1] The CFAA's "exceeded authorized access" provision is inapplicable in this matter. See Van Buren v. United States, --- S.Ct. ----, No. 19-783, 2021 WL 2229206, at *12 (U.S. June 3, 2021) ("In sum, an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him.") Although the Supreme Court addressed "exceeds authorized access" in the § 1030(a)(2) context, the Court finds no reason to apply a different interpretation to Plaintiff's § 1030(a)(4) claim. Here, the parties' arguments do not concern exceeding authorized access-- Defendant claims that it was fully entitled to access Plaintiff's phone, and Plaintiff argues that Defendant had no authorization whatsoever. If discovery reveals contradictory information, Defendant may raise this argument again in a future motion.

In response, Plaintiff contends that Defendant's authority to access his smart phone, to the extent that authority ever existed, terminated once his employment ended. So, because Plaintiff was no longer an employee of Defendant at the time of the access to his smart phone, that access was unauthorized.

As an initial matter, the Court cannot consider the Employee Handbook at this juncture because it is an extraneous document to the Complaint. See In re Burlington Coat Factory Sec. Litig., 114 F.3d 1410, 1426 (3d Cir. 1997) ("[A] district court ruling on a motion to dismiss may not consider matters extraneous to the pleadings."). But Plaintiff's Employment Agreement is a "document integral to or explicitly relied upon in the complaint," which the Court may consider. Id.

Here, whether Plaintiff was obligated to return certain business data stored on his smart phone is irrelevant to his CFAA claim. This claim concerns authorization to access. Possession of another's property is not authorization for the property-owner to reclaim possession by any means necessary.

Moreover, Plaintiff clearly alleges that Defendant lacked authorization to access his iPhone, which Defendant has not sufficiently disputed. Defendant's arguments generally pertain to Plaintiff's employer-provided e-mail address. But that is not in dispute. Stated differently, Plaintiff does not allege an unauthorized access of his e-mail address, he alleges that

Defendant, without authorization, accessed his smart phone, "which was [Plaintiff's] personal property and not issued or owned by [Defendant.]" [Docket No. 1, at ¶ 25]. Although Defendant may establish that Plaintiff consented to access, Plaintiff has sufficiently alleged that Defendant's access, at this juncture, was done without authorization.

C. Knowingly and with Intent to Defraud

As noted above, a plaintiff must establish that the defendant accessed his computer "knowingly" and with "intent to defraud." P.C. Yonkers, Inc., 428 F.3d at 508. Although Defendant seemingly argues that it did not access Plaintiff's smart phone "knowingly," [Docket No. 9-1, at 4] ["The Plaintiff has failed to allege that the Defendant 'knowingly' . . . undertook the conduct complaint of."], the Court dismisses such argument. Defendant's brief raises no argument that it accessed Plaintiff's phone negligently or accidentally, and it fails to provide any other argument showing that its access was made unknowingly.

As to the "intent to defraud" element, Defendant likewise argues that Plaintiff has failed to allege any facts that satisfy this criterion. Plaintiff responds that Defendant used fraud and deceit to access his smart phone. More specifically, Plaintiff alleges that Defendant accessed his phone by using "an e-mail [account] associated with Plaintiff's Apple ID to reset

Plaintiff's password to Plaintiff's 'find my iPhone' account in order to access such account for the purpose of deleting data from Plaintiff's iPhone." [Docket No. 13, at 10]. This, Plaintiff contends, was an intent to defraud because Defendant deceived "Apple, Inc. into believing that it was Plaintiff attempting to access the account." [Id.].

"Intent to defraud," as relevant here raises two questions: (1) what constitutes "intent to defraud" under the CFAA, and (2) does the CFAA require the plaintiff to be the victim of fraud. Some courts have explained that "defraud," as used in CFAA § 1030(a)(4), means "'wronging one in his property rights by dishonest methods or schemes.'" Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000). For example, in Shurgard, the Western District of Washington held that "the CFAA's use of 'fraud' simply means wrongdoing and not proof of the common law elements of fraud." Id. at 1126.

The Third Circuit has neither adopted nor rejected this definition. But it has been widely adopted by district courts across the country. See e.g., SMH Enterprises, L.L.C. v. Krispy Krunchy Foods, L.L.C., No. CV 20-2970, 2021 WL 1226411, at *5 (E.D. La. Apr. 1, 2021); TracFone Wireless, Inc. v. Cabrera, 883 F. Supp. 2d 1220, 1227 n.2 (S.D. Fla. 2012); Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc., 556 F. Supp. 2d

1122, 1131 (E.D. Cal. 2008); NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1062 (S.D. Iowa 2009). Moreover, and as recognized by the First Circuit in United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997), Congress used § 1030(a)(4)'s "intent to defraud" language synonymously with "wrongfully." Czubinski, 106 F.3d at 1078 (citing 132 Cong. Rec. 7128, 7129, 99th Cong., 2d. Sess. (1986) and S. Rep. No. 432, 99th Cong., 2d Sess., reprinted in 1986 U.S.C.C.A.N. 2479, 2488.) Therefore, the Court will apply the Shurgard definition of fraud.

As alleged in the Complaint, Defendant purportedly used dishonest means to reset Plaintiff's Apple ID password and access his account. That Plaintiff has not alleged common law fraud is irrelevant. Under Shurgard, Plaintiff has sufficiently alleged that Defendant acted with "intent to defraud" pursuant to the CFAA.

As noted above, there is also a question of whether the CFAA requires Plaintiff to be the victim of Defendant's purported fraud. The parties have identified no caselaw establishing that a plaintiff cannot maintain a CFAA claim when the defrauded-party was a third-party to the litigation. In addition, the CFAA does not explicitly state that Plaintiff must be the victim of such fraud. See § 1030(a)(4) ("whoever . . . knowingly and with intent to defraud . . ."). The Court notes, however, that the CFAA is primarily a criminal statute, so this

information was largely unnecessary until the addition of subsection (g).

Nevertheless, § 1030(g) does not require the plaintiff to be the fraud victim. Instead, subsection (g) only requires the plaintiff to suffer "damage or loss" due to the defendant's violation of the CFAA. A plain reading of the statute permits a plaintiff to bring a CFAA action, regardless of who the defrauded-party may be, so long as that plaintiff sufficiently alleges damage or loss. Thus, Plaintiff's argument that Defendant committed fraud, under the CFAA, by deceiving Apple and impermissibly accessing his Apple ID is sufficient to establish this element of the CFAA.

D. Furthered the Fraud and Obtained Anything of Value

The next element of the CFAA requires Plaintiff to show that Defendant further the intended fraud and obtained anything of value. P.C. Yonkers, Inc., 428 F.3d at 508.

In a typical CFAA case, particularly one related to employment, this element is rarely in dispute. In these cases, a plaintiff-employer usually alleges that an employee or former employee downloaded certain files, see e.g., Dresser-Rand Co., 957 F. Supp. 2d at 611, or acquired trade secrets and other confidential information. See e.g., Teva Pharms. USA, Inc. v. Sandhu, 291 F. Supp. 3d 659, 667 (E.D. Pa. 2018).

But this is not a typical CFAA case, and this element is disputed. For Plaintiff to satisfy this element, he must establish that Defendant engaged in conduct to further its alleged fraud, that it "obtained" something, and that what it obtained has some "value."

As a preliminary matter, the Court notes that Defendant has not argued this specific point. Instead, Defendant primarily contends that Plaintiff has not suffered damage or loss under the CFAA, and that it had authorization to access Plaintiff's iPhone. Nevertheless, the Court finds that Defendant has broadly challenged Plaintiff's entire CFAA claim and that there is significant interplay between Defendant's arguments and this element, such that it is appropriate to consider this issue now.

As alleged in the Complaint, Defendant-- after it deceived Apple into providing Plaintiff's Apple ID-- used Plaintiff's login information to access his iPhone and to gain the necessary permissions to remotely delete Plaintiff's data. At this stage in the case, Plaintiff has satisfied this element of the CFAA.

Plaintiff clearly alleges that Defendant used the information it gained through deceit to access his phone. Defendant then allegedly obtained the ability to remotely delete Plaintiff's data. Although there may be a question of whether the ability to delete data is something "of value," discussed more thoroughly below, this ability was "obtained" through

Defendant's alleged fraud. Therefore, Plaintiff satisfies both the "further the fraud" and "obtained" factors of this element.

Finally, the ability to remotely delete data constitutes something of "value." Both the First and Tenth Circuits define "anything of value" as: "relative to one's needs and objectives." Triad Consultants, Inc. v. Wiggins, 249 F. App'x 38, 41 (10th Cir. 2007); Czubinski, 106 F.3d at 1078. The Court will adopt this definition. Given Plaintiff's allegations that Defendant obtained the ability to remotely delete his data and that Defendant's goal was to delete data, the Court finds that, relative to Defendant's purported objective, Plaintiff has alleged that Defendant obtained something of value.

E. Damage or Loss in Excess of $5,000

A plaintiff must allege that the defendant's actions, in violating the CFAA, "caused damage or loss to the plaintiff in excess of $5,000 in a one-year period." Teva Pharms. USA, Inc., 291 F. Supp. 3d at 668 (quoting 18 U.S.C. § 1030(a)(4)). "Loss," under the CFAA, refers to "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." § 1030(e)(11). "Numerous district court decisions in the Third Circuit have

held that to fall within this definition of 'loss,' the 'alleged loss must be related to the impairment or damage to a computer or computer system.'" Sealord Holdings, Inc. v. Radler, No. CIV.A. 11-6125, 2012 WL 707075, at *4 (E.D. Pa. Mar. 6, 2012) (collecting cases).

So, a compensable loss under the CFAA is generally either "the cost of remedial measures taken to investigate or repair the damage to the computer, or . . . the amount of lost revenue resulting from a plaintiff's inability to utilize the computer while it was inoperable because of a defendant's misfeasance." Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio, No. CIV.A. 09-2751, 2011 WL 6088611, at *5 (E.D. Pa. Dec. 7, 2011). Stated differently, the "loss" must generally be "in some way related to functionality of the protected computer at issue." Id.

The CFAA also permits a Plaintiff to recover for "damage." The CFAA defines damage as "any impairment to the integrity or availability of data, a program, a system, or information." § 1030(e)(8). Indeed, some courts have held that "[p]ermanent deletion of files from a laptop computer without authorization . . . may constitute 'damage' under the CFAA." Calkins v. IPD Analytics, L.L.C., No. 08-23188-CIV-MORE, 2009 U.S. Dist. LEXIS 85702, at *17 (S.D. Fla. Apr. 16, 2009).

Here, Plaintiff argues that the "business interruption and the loss of [] data and records result[ed] in monetary damages valued at more than $10,000.00." [Docket No. 1, at ¶ 54]. Defendant responds that Plaintiff has not suffered a cognizable "loss" or "damage," and that Plaintiff's alleged loss of personal data cannot meet the CFAA's "in excess of $5,000" requirement.

Defendant's arguments are unpersuasive. Plaintiff has clearly alleged "damage" under the CFAA. Due to Defendant's alleged actions, Plaintiff argues that his data and information is no longer available, which satisfies the CFAA definition. In addition, the CFAA establishes that "loss" includes "responding to an offense . . . and restoring the data, program, system, or information to its condition prior to the offense. § 1030(e)(11). As stated in the Complaint, Plaintiff alleges that he has attempted to retrieve and recover the lost data. [Docket No. 1, at ¶ 28]. Moreover, the Court is also satisfied that Plaintiff's smart phone suffered a loss of functionality. To the extent that Plaintiff used his phone as a storage device for his pictures and videos, and as a contact list for phone numbers, Plaintiff has alleged a loss of functionality. Therefore, Plaintiff has claimed both "loss" and "damages" under the CFAA.

The final issue concerns the monetary loss of Plaintiff's claim. When reviewing a challenge to a plaintiff's asserted

damages amount, the Court "consult[s] the face of the complaint and accept[s] the plaintiff's good faith allegations." Vasvari v. Hartung, No. 16-6461-BRM-TJB, 2017 WL 6417633, at *2 (D.N.J. Dec. 15, 2017) (citing Frederico v. Home Depot, 507 F.3d 188, 194 (3d Cir. 2007)). "[T]he sum claimed by the plaintiff controls if the claim is apparently made in good faith." Suber v. Chrysler Corp., 104 F.3d 578, 583 (3d Cir. 1997) (citation omitted). The Court will dismiss an action for failure to meet the jurisdictional amount if the Court "is certain that the jurisdictional amount cannot be met." Id. (citing Columbia Gas Transmission Corp. v. Tarbuck, 62 F.3d 538, 541 (3d Cir.1995)). This is often described as the legal certainty test. Id. Similarly, the Third Circuit has also held that that courts should dismiss for lack of jurisdiction in federal question cases when claims are "insubstantial on their face." See id. (citing Lunderstadt v. Colafella, 885 F.2d 66, 69–70 (3d Cir.1989)).

Under both the "legal certainty" test and the "insubstantial on [its] face" test, the Court is satisfied that Plaintiff has alleged more than $5,000 in damages. Some of Plaintiff's allegedly lost data may be easier to quantify than others-- for example, Plaintiff's lost "purchased apps" [Docket No. 13, at 10] are far easier to assess than Plaintiff's lost pictures and videos. In any event, Plaintiff's claim of $10,000

in lost data is not unreasonable on its face, and the Court cannot infer bad faith or insubstantiality. Defendant has also failed to offer any substantive challenges to Plaintiff's claim. At most, Defendant's argument is simply that it believes Plaintiff assess his lost data too highly. This is insufficient. Thus, the Court finds that Plaintiff has stated a claim under the CFAA.

F. Supplemental Jurisdiction

Having found that Plaintiff has stated a claim under the CFAA, the Court will not dismiss Plaintiff's remaining claims for lack of subject matter jurisdiction. In addition, the Court will exercise jurisdiction over Plaintiff's related state law claims.

IV. CONCLUSION

Thus, for the foregoing reasons, the Court will DENY Defendant's Motion to Dismiss [Docket No. 9]. An appropriate Order accompanies this Opinion.

Dated: June 15, 2021

s/Renée Marie Bumb
RENÉE MARIE BUMB
United States District Judge